HARTING Vending GmbH & Co. KG
Marienwerderstr. 3
D-32339 Espelkamp

2000-07-30
200-14 EP P 4

Verfahren für eine sichere Datenübertragung beim Warenverkauf

Die Erfindung betrifft ein Verfahren für eine sichere Datenübertragung beim Warenverkauf, wobei ein Warenauswahlterminal sowie eine Kasseneinrichtung mit einer Beleglesestation und ein Warenausgabespeicher vorgesehen sind, und wobei an dem Warenauswahlterminal eine Ware ausgewählt wird und mittels einer Druckereinrichtung ein Beleg für die gewählte Ware ausgegeben wird.

Beim Kauf von Waren und hierbei speziell höherwertiger Waren, bei dem die Auswahl und die Ausgabe der Waren in unterschiedlichen räumlichen Bereichen abgewickelt wird, ist eine fälschungssichere Übermittlung der Warendaten von deren Erfassung bis zur berechtigten Warenausgabe erforderlich.

Aus der DE 42 17 045 A1 ist ein Verfahren zum Verkauf von Waren bekannt, bei dem die Waren in einem Warenausgabeautomaten gelagert sind, und wobei mindestens ein Warenauswahlterminal sowie eine Kasse vorgesehen sind. Bei der Auswahl der Waren aus dem Warenauswahlterminal wird ein auswahlspezifisches Signal generiert. Nach Bezahlung des Warenwertes wird von der Kasse ein Kaufbeleg erzeugt, der einer Lesevorrichtung des Warenausgabeautomaten zugeführt wird und eine Ausgabe der entsprechende Ware aus dem Warenausgabeautomaten auslöst.
Weiterhin ist aus der DE 695 04 729 T2 einer Übersetzung der EP 0 670 132 B1 eine Vorrichtung zur Bereitstellung von Cigarettenpackungen an einer Vielzahl von Kassentischen bekannt, wobei die Vorrichtung einen zentralen Lagerraum aufweist, sowie Mittel, aufgestellt auf dem Kassentisch, mit

denen eine Auswahl der Packungsarten getroffen werden kann, sowie ein Transportsystem zur Zuführung der Packungen zum Kassentisch.

Nachteilig wirkt sich bei den bekannten Verfahren aus, dass entweder aufwendige Transportsysteme vorgesehen sein müssen, oder dass die Kaufbelege eine unzureichende Sicherung gegen Mißbrauch speziell bei höherwertigen Waren aufweisen.

Dieser Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren der eingangs genannten Art dahingehend auszubilden, dass ein oder mehrere Belege, bzw. Informationsträger zur Warenidentifikation mit nachahmungssicheren Maßnahmen versehen sind, die eine berechtigte Warenausgabe sicherstellen.

Diese Aufgabe wird dadurch gelöst, dass der Beleg mit einem ersten selbstprüfenden Verschlüsselungskode und mit einem ersten Algorithmus zur Verschlüsselung der Warenidentifikation der gewählten Ware oder der Verkaufsidentifikation eines Verkaufsvorganges versehen wird, wobei sich auf dem Beleg eine oder mehrere Verkaufsidentifikationen befinden, dass die Verschlüsselung auf dem Beleg an der Beleglesestation identifiziert (entschlüsselt) wird, wobei der der Ware zugehörige Wert ermittelt und zum Wertausgleich (Bezahlung) an die Kasseneinrichtung weitergeleitet wird, dass nach Bezahlung der Ware die Kasseneinrichtung mittels einer damit verbundenen Ausgabevorrichtung einen elektronischen Informationsträger ausgibt, wobei der elektronische Informations-träger eine CPU enthält, die mindestens einen zweiten, selbstprüfenden Verschlüsselungskode beliebiger Verschlüsselungs-tiefe mit einem zweiten Algorithmus zur Verschlüsselung für die gesamte bezahlte Ware generiert, wobei der zweite Verschlüsselungskode unterschiedlich oder auch gleich zum ersten Verschlüsslungskode ist, und dass der elektronische Informationsträger einer Leseeinheit im Warenausgabespeicher zur Identifikation und zur Entschlüsselung des zweiten Verschlüsselungskodes zugeführt wird, wobei

bei einer zulässigen Identifikation die Ausgabe der gewählten Ware in der gewählten Menge aus dem Warenausgabespeicher ausgelöst wird.

Vorteilhafte Ausgestaltungen der Erfindung sind in den Ansprüchen 2 - 5 angegeben.

Die mit der Erfindung erzielten Vorteile bestehen insbesondere darin, dass vorzugsweise ein Warenverkauf mit mindestens zwei bezüglich ihrer Speicherform unabhängigen Informationsträgern getätigt wird, wodurch eine sichere, berechtigte Warenausgabe gewährleistet ist.
Dabei wird vorteilhafterweise die gewünschte Ware von einem Kunden an einem elektronischen Warenauswahlterminal ausgewählt, das innerhalb eines Warenangebotsbereiches angeordnet ist. Mittels einer Druckervorrichtung, die dem Warenauswahlterminal zugeordnet ist, wird als Informationsträger ein Beleg ausgegeben, der die gewählte Ware für den Kunden in Klarschrift ausgibt sowie gleichzeitig eine kodierte und selbstprüfende Verschlüsselung aufweist, die idealerweise durch einen Belegleser zu entschlüsseln ist.
Nach dem Bezahlen der Ware in einem Kassenbereich wird mittels einer Ausgabevorrichtung, angeordnet in unmittelbarer Kassennähe, ein elektronischer Informationsträger an den Kunden ausgegeben.
Dieser Informationsträger kann vorteilhafterweise als Transponder, als münzähnlicher Chip, oder als Chip-Karte auch Smart-Card genannt, ausgeführt sein. Der Informationsträger enthält in einem Fall vorteilhafterweise einen Rechnerbaustein (CPU), der selbsttätig einen selbstprüfenden Verschlüsselungskode mit einem Algorithmus erzeugt.
In einem anderen Fall enthält die Ausgabeeinrichtung einen Rechnerbaustein (CPU), die den Verschlüsselungscode erzeugt, der dann in einem als passiven Speicher ausgerüsteten Informationsträger abgespeichert wird, dieser ist gegebenenfalls durch einen mehrstelligen PIN vor unerwünschtem Auslesen geschützt.
Der Informationsträger mit den verschlüsselten Warendaten wird einer Leseeinheit in einem außerhalb des Warenangebotsbereiches angeordneten

Warenausgabespeicher zur Entschlüsselung zugeführt, die nach einer Plausibilitätsprüfung mit Hilfe des entsprechenden Algorithmus f_2, f'_2 , die Ausgabe der ausgewählten Ware aus einem Warenausgabespeicher auslöst.

Der Informationsträger verbleibt zunächst vorteilhafterweise im Warenausgabespeicher und kann jederzeit nach einer Rückführung zum Kassenbereich mit einer neuen Verschlüsselung versehen werden.
Weiterhin besteht der Vorteil bei einer Warenausgabe aus dem Warenausgabespeicher, dass bei zusätzlichen, erforderlichen Sicherheitsüberprüfungen, wie z. B. bei der Abgabe von Alkohol oder Cigaretten gemäß den gesetzlichen Vorschriften für den Jugendschutz, eine Sperrung der Warenausgabe durch eine authorisierte Aufsichtsperson erfolgen kann.
Damit kann z. B. eine Personenkontrolle vom Kassenpersonal auf eine Sicherheitsperson verlagert werden.
Weiterhin kann eine Berechtigungsüberprüfung bereits aufgrund einer Kodierung der Ware bei der Auswahl im Warenauswahlterminal enthalten sein.
Das Verfahren bietet sich vorteilhafterweise insbesondere auch für Kassenbereiche an, bei denen der Kunde bereits selbsttätig die Identifikation der Ware für den Bezahlvorgang vornehmen kann.
Weiterhin kann eine verschlüsselte Datenübertragung mittels kabelloser oder kabelgebundener Datenübertragung vorteilhaft zwischen dem Warenausgabespeicher und dem Warenauswahlterminal gegen eine externe Datenmanipulation (Hackerangriff) eingesetzt werden.

Ein Ausführungsbeispiel der Erfindung ist in der Zeichnung dargestellt und wird im folgenden näher erläutert. Es zeigen:

Fig.1 eine schematische Darstellung des Verfahrens zur sicheren Datenübertragung beim Warenverkauf und

Fig. 2 eine Erläuterung für das Verschlüsselungsverfahren

In der Fig.1 ist in einer schematischen Darstellung das Verfahren zur sicheren Datenübertragung beim Warenverkauf gezeigt.
Dabei ist der gesamte Verkaufsbereich in drei Bereiche unterteilt: einem Warenangebotsbereich 1, einem Kassenbereich 2 und einem Warenausgabebereich 3.
Mittels eines Warenauswahlterminals 10, das räumlich innerhalb des Warenangebotsbereiches 1 angeordnet ist, werden verschiedene Waren ausgewählt, wobei ein an das Warenauswahlterminal angeschlossener Belegdrucker 14 einen Beleg 16 ausgibt.
Dabei ist das Warenauswahlterminal datentechnisch mit einem oder mehreren im Warenausgabebereich 3 angeordneten Warenausgabespeichern 30 verbunden.
Der Beleg 16 enthält als Informationsträger die gewählte Ware im Klartext, sowie eine Verschlüsselung von mindestens Art und Menge der Ware.
Die Verschlüsselung wird gegebenenfalls aus einer Zufallszahl bzw., selbstprüfenden Zahl P und einem Algorithmus f_1 gebildet und wird durch einen im Warenauswahlterminal 10 vorgesehenen Rechnerbaustein CPU 12 gebildet und ausgegeben.
Dabei kann die Warenidentifikation oder auch eine Verkaufsidentifikation eines Verkaufsvorganges zur Verschlüsselung herangezogen werden.

Der Beleg kann idealerweise in Papierform ausgegeben werden und wird bei Verlassen des Warenangebotsbereiches 1 von einem Belegleser 22 in der Kasseneinrichtung 20 identifiziert und einbehalten.
Nach einem Wertausgleich dieser oder auch weiterer nicht über das Warenauswahlterminal georderter Ware durch eine Barzahlung oder bargeldlose Zahlung, gibt eine im Kassenbereich 2 angeordnete Ausgabeeinrichtung 24 einen weiteren Informationsträger 26 aus, der jedoch eine eigene CPU 28 enthält, die selbsttätig mittels einer selbstprüfenden Zahl P' und einem Algorithmus f'_1, f'_2 eine Verschlüsselung der bezahlten Waren vornimmt.
Dabei kann der Informationsträger 26 als Transponder, einzelner Chip oder Chipkarte (Smartcard) ausgebildet sein.

In einer Variante kann jedoch auch die Ausgabeeinheit 24 eine CPU 28' enthalten, die eine Verschlüsselung vornimmt und diese einem passiven als Speicher ausgebildeten Informationsträger 26' übermittelt.
Dabei kann die Verschlüsselung zusätzlich mit einer gegebenenfalls mehrstelligen PIN-Nummer versehen sein.
Im Warenausgabebereich 3 wird der Informationsträger 26, 26' einer Leseeinheit 32 des Warenausgabespeichers 30 zugeleitet, die die verschlüsselten Informationen dekodiert und eine Ausgabe der ausgewählten Waren 40 einleitet.
Die Informationsträger verbleiben bis zu einer erneuten Verwendung im Warenausgabespeicher.

In diesem Beispiel wird ein Verfahren beschrieben, bei dem mindestens zwei unabhängige Verschlüsselungsverfahren genutzt werden, dies ist jedoch nicht unbedingt zwingend, da jedes Verschlüsselungsverfahren auch einzeln einsetzbar ist.

Erläuterungen zum Verfahren für die Verarbeitung und Validierung der selbstprüfenden Daten mit Hilfe einer selbstprüfenden Zahl P_i, welche Informationen zum Kauf und zur Berechtigung hinsichtlich der Sorte der gewünschten Ware und deren Menge hinsichtlich der Ausgabe an der Ausgabeeinrichtung 30, und der Möglichkeit zur Kodierung einer logischen Fortfolge in einem bestimmten Teil der enthaltenen Stellen enthält.

Verfahren:
Bei der Verschlüsselung, zwecks Selbstprüfung und Berechtigungsprüfung für den Bediener (Endkunden), handelt es sich um die eine Berechnungsvorschrift (Algorithmus f_2) welche die aus *m* Stellen bestehenden Zahl X_1 in die Zahl Y_1 überführt, die idealerweise aber nicht zwingend, auch aus *m* Stellen besteht.
Diese Verschlüsselung sowie das Prüfungsverfahren kann beim Warenauswahlterminal zur Erstellung des Beleges mit einer selbstprüfenden Zahl P sowie bei dem als Chipkarte ausgeführten Informationsträger 28, an

der Ausgabevorrichtung im Kassenbereich mit der selbstprüfenden Zahl P' erfolgen.

Dabei ist es unerheblich ob es sich in den Fällen um die jeweils gleichen oder unterschiedlichen Algorithmen f_1 und f_2 (oder eben f'_1 und f'_2 mit $f'_1 \neq f_1$ und f'_2 mit $f'_2 \neq f_2$) handelt. Eine Unterscheidungen der beiden Algorithmen ist jedoch nicht für die Selbstprüfung zwingend, insofern könnten diese auch beide gleich sein.

In der in Fig. 2 dargestellten Schreibweise, bilden die beiden Zifferngruppen der Zahl X_1 und der Zahl Y_1 gemeinsam die gewünschte selbstprüfende Kodierungszahl P_1 (beziehungsweise P'_1).

Der Verschlüsselungsalgorithmus f (also f_1, f_2, f'_1, f'_2) jeweils an sich, kann ein beliebiger sein. Insbesondere jeder bekannte, z. B. DES(-RSA), Rijndael, Eliptic Curves, o.dgl. oder auch jeder neuentwickelte Verschlüsselungsalgorithmus oder dergleichen kommt hierbei in Frage, insofern er eindeutig in Bezug auf die aus der eingangsseitig eingegebenen Zahl X_1 berechneten Zahl Y_1 ist und somit die gewünschte selbstprüfende Kodierungszahl P_1

z. B. durch „Zusammensetzung" der Stellen in der Reihenfolge „XY" bildet, oder gegebenenfalls durch eine weitere Berechnung ineinander überführt. Dabei enthält X unter Umständen die höherwertigen und Y enthält die niederwertigen Stellen der Zahl P, aber auch die umgekehrte Reihenfolge (X = niederwertige Stellen / Y = höherwertige Stellen) ist dabei denkbar. Dabei ist die Anzahl der Stellen *m* zur Basis der Ziffern hinreichend groß zu wählen.

Idealerweise sind 20 Stellen vorgesehen, aber auch mehr oder weniger Stellen unter Verwendung von Ziffern, wie auch alphanumerischen Zeichen (A-Z; a-z) wie auch Sonderzeichen sind im Rahmen der Kodierungstiefe vorsehbar. Vorsehbar im Sinne der Informationstechnik, verstanden als Anzahl der verwendeten „Bits-pro-Zeichen" der verwendeten Stelle, insbesonder dazu verwendet um eine ausreichende Sicherheit gegen „Zufallstreffer" zu gewährleisten. Der Begriff „Zahl" ist somit also nur ein

„Platzhalter" für jede anwendbare Informationseinheit im mathematischen Sinne.

Plausibilitätskontrollalgorithmus f_1 zwischen den erzeugten Verkaufsinformationen im Sinne einer „Fortfolge"-Plausibilität:
Ebenso wird eine zweite von der ersten hinsichtlich des Algorithmus unabhängig (oder gegebenenfalls auch identisch) vorliegende Verschlüsselungsfunktion f_2 gebildet, welche ausschließlich aus einer eingegebenen Zahl X_1 eine nachfolgende Zahl X_2 in der gleichen eindeutigen Weise bildet. Wobei darüber hinaus aus der Zahl X_2 in der gleichen eindeutigen Weise eine Zahl X_3 gebildet werden kann. Diese Zahlenfolge A die dabei als eineindeutige und reproduzierbare Folge A entsteht, dient dann jeweils in ihren Einzelwerten als Argument X_i der nachfolgenden Funktion f_2 zur Erzeugung der oben gewünschten Zahl P_i.
Dabei kann oder muss lediglich ein Teil der verwendeten Stellen innerhalb dieser Zahl X_i zur Plausibilitätskontrolle gegenüber der Zahl $X_{(i-1)}$ mit Hilfe des Algorithmus f_1 verwendet werden.

Der Zweck dieser Plausibilitätskontrolle ergibt sich aus der Betrachtung eines denkbaren Betrugsverfahrens, in dem ein Endkunde in betrügerischer Absicht, durch ein technisch nicht unmögliches, wenngleich sehr schwieriges Kopieren des Informationsträgers, welcher durch die CPU 28 beschrieben wird, versuchen könnte, eine durch diesen Kopiervorgang entsprechend der Menge der kopierten und somit vervielfältigten Informationsträgereinheiten entsprechenden Anzahl von Waren, nach dem Verlassen der Kasse und dem vorausgegangenen Bezahlen einer einzelnen Informationsträgereinheit an derselben, dann unbeaufsichtigt an der Warenausgabeeinheit erhalten könnte.
Die Einzigartigkeit der verkaufsrelevanten Information in der CPU 28 im Rahmen der Fortfolge des geheimen Algorithmus f_1, f_2 ist somit wesentlicher und nicht trennbar Bestandteil dieses Verfahrens.

Die Reproduzierbarkeit der über den geheimen Algorithmus f_1 in den relevanten Stellen erzeugten Fortfolge A ist somit ebenso ein relevanter Bestandteil und untrennbar mit dem Verfahren verbunden.

Informationsspeicherungsmöglichkeiten innerhalb der Zahl X:
Ein anderer Teil der Stellen der jeweiligen Zahl X_i kann bzw. muss zum Aufnehmen der Informationen über die gewählte Sorte und die gewählte Menge dieser Sorte und gegebenenfalls zusätzlicher Informationen wie z. B. den Jugendschutz verwendet werden, jedoch ohne die Notwendigkeit der Einbeziehung dieser weiteren Stellen für die Plausibilitätskontrolle hinsichtlich der verwendeten Algorithmen f_1 und f'_1.
Es ist dabei nicht erforderlich, allerdings auch nicht undenkbar und somit auch anwendbar, dass diese Informationen, welche für die Ausführung und Prüfung durch den Algorithmus f_1 (f'_1), irrelevant sind, in sich wiederum verschlüsselt werden. Allerdings können diese auch im Klartext, wie im Beispiel angeführt, dargestellt werden.

Ebenso gibt es keine zwingende Vorgabe über das Verhältnis der Stellenanzahl derjenigen Informationen innerhalb der Zahl X im Verhältnis zur Stellenanzahl der Informationen der Plausibilitätskontrolle durch den Algorithmus f_1 (f'_1) für die korrekte Fortfolge der Zahlen X_i, welches also ein beliebiges Verhältnis sein kann, in soweit dann auch noch eine hinreichend sichere Verwendung der Plausibilitätskontrolle durch den Algorithmus f_1 (f'_1), möglich bleibt.
Ebenso ist es allerdings denkbar, dass dieses Verfahren auch für feststehende Mengen und feststehender Sortencodes angewendet werden kann, insofern dann keine Notwendigkeit zur Übertragung von Mengen oder Codes oder weiteren beliebigen Informationen erforderlich ist, sondern lediglich eine einzige Ware in einer Einzelstückzahl verkauft werden soll.
In diesem Sonderfall können also alle Stellen der Zahl X vollständig zur Plausibilitätskontrolle hinsichtlich des Algorithmus f_1 (f'_1), Verwendung finden.

Schemata:

Die fortlaufende Anwendung dieses Schemata führt zur Prüfzahlenfolge P. Dieses Schemata kann gemäß der Funktionen f_1 und f_2 (also auch f^{l}_1, f^{l}_2)universell beschrieben werden:

Speziell: $Y_1 = f_2(X_1)$ / Allgemein: $Y_n = f_2(X_n)$: -> P_1={„X_1Y_1"}
Speziell: $X_2 = f_1(X_1)$ / Allgemein: $X_{(n-1)} = f_2(X_n)$: -> X_i
jeweils als Argument für f(x)

Als „Startzahl" (Initialzahl) für dieses Schemata kann, muss jedoch nicht zwingend, eine bewusst durch den Betreiber gewählte Zahl X_0 existieren, die insoweit gewünscht eine Möglichkeit bietet, die Reproduzierbarkeit der Zahlenfolge A über den jeweiligen Algorithmus f in CPU 12 bzw. CPU 28 zu gewährleisten. Als Alternative könnte auch eine zufällige computergenerierte Zahl stehen, über deren Kenntnis weder der Betreiber noch ein Servicetechniker noch ein Mensch im allgemeinen verfügen müsste.
Bei gleicher „Startzahl" sowohl in der erzeugenden CPU12 als auch in der zweiten prüfenden CPU 28 und jeder weiteren CPU lässt sich eine einfache weitere Sicherheitsfunktion im Rahmen einer „Plausibilitätskontrolle" realisieren:
Gleiche Startzahlen führen bei gleichen Algorithmen zu gleichen Zahlenfolgen A, somit zu gleichen Prüfzahlenfolge P im Rahmen der oben erwähnten relevanten Stellen der Zahlenfolge A (X_i) selbstverständlich ausschließlich bezogen auf die verwendeten relevanten Stellen für die Plausibilitätskontrolle der Fortfolge gemäß dem Algorithmus f_1 (f^{l}_1).
Als besonders vorteilhafter Ausprägung der Erfindung ergibt sich damit die universelle Möglichkeit sowohl zur Kodierung von Informationen in Bezug auf ausgewählte Mengen und gewählte Warenarten innerhalb der Zahlen P_i, als auch zur Prüfung der Konsistenz fortlaufender Zahlenfolgen zur Verhinderung des Betrugs und des Missbrauches durch Kunden in Bezug auf die Wiederverwendung schon einmal verwendeter Zahlenfolgen, unter der Voraussetzung der Gleichheit der Initialzahl („Startzahl") in allen CPU Instanzen innerhalb der Zahlenfolge A.

Unter der Voraussetzung der Gleichheit der Initialzahl in den CPU's, kann jeder somit einzigartig erzeugte Beleg bzw. Informationsträger, erzeugt in CPU 12 sowie im Informationsträger CPU 28 nur ein einziges Mal in dieser Form zum Verkauf erzeugt und auch verwendet werden.

Bestätigungskopie

HARTING Vending GmbH & Co. KG
Marienwerderstr. 3
D-32339 Espelkamp

2000-07-30
200-14 EP P 4

Verfahren für eine sichere Datenübertragung beim Warenverkauf

Patentansprüche

1. Verfahren für eine sichere Datenübertragung beim Warenverkauf, wobei ein Warenauswahlterminal (10) sowie eine Kasseneinrichtung (20) mit einer Beleglesestation (22) und ein Warenausgabespeicher (30) vorgesehen sind, und wobei an dem Warenauswahlterminal (10) eine Ware ausgewählt wird und mittels einer Druckereinrichtung (14) ein Beleg (16) für die gewählte Ware ausgegeben wird, dadurch gekennzeichnet,
dass der Beleg (16) mit einem ersten selbstprüfenden Verschlüsselungskode (P) und mit einem ersten Algorithmus (f_1, f_2) zur Verschlüsselung der Warenidentifikation der gewählten Ware oder der Verkaufsidentifikation eines Verkaufsvorganges versehen wird, wobei sich auf dem Beleg eine oder mehrere Verkaufsidentifikationen befinden,
dass die Verschlüsselung auf dem Beleg (16) an der Beleglesestation (22) identifiziert (entschlüsselt) wird, wobei der der Ware zugehörige Wert ermittelt und zum Wertausgleich (Bezahlung) an die Kasseneinrichtung (20) weitergeleitet wird,
dass nach Bezahlung der Ware die Kasseneinrichtung (20) mittels einer damit verbundenen Ausgabevorrichtung (24) einen elektronischen Informationsträger (26) ausgibt, wobei der elektronische Informationsträger eine CPU (28) enthält, die einen zweiten, selbstprüfenden Verschlüsselungskode (P') beliebiger Verschlüsselungstiefe mit einem zweiten Algorithmus (f'_1, f'_2), zur Verschlüsselung für die gesamte bezahlte Ware generiert, wobei der

zweite Verschlüsselungskode unterschiedlich oder auch gleich zum ersten Verschlüsslungskode ist, und
dass der elektronische Informationsträger (26) einer Leseeinheit (32) im Warenausgabespeicher (30) zur Identifikation und zur Entschlüsselung des zweiten Verschlüsselungskodes (P') zugeführt wird, wobei bei einer zulässigen Identifikation die Ausgabe der gewählten Ware (34) in der gewählten Menge aus dem Warenausgabespeicher (30) ausgelöst wird.

2. Verfahren für eine sichere Datenübertragung beim Warenverkauf nach Anspruch 1, dadurch gekennzeichnet,
dass die Ausgabevorrichtung (24) eine CPU (28') enthält, die den zweiten selbstprüfenden Verschlüsselungskode (P') mit einem zweiten oder gleichen Algorithmus (f_1, f_2, f'_1, f'_2) zur Verschlüsselung für die bezahlte Ware generiert, wobei der elektronische Informationsträger (26') als passiver Speicher ausgebildet ist, und wobei zusätzlich eine PIN-Nummer eingefügt wird.

3. Verfahren für eine sichere Datenübertragung beim Warenverkauf nach Anspruch 1 oder 2, dadurch gekennzeichnet,
dass in einer Variante der erste Algorithmus (f_1, f_2) keinen Verschlüsselungsalgorithmus darstellt und somit auch keine Verschlüsselung des Beleges (16) angewandt wird.

4. Verfahren für eine sichere Datenübertragung beim Warenverkauf nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass eine verschlüsselte Datenübertragung zwischen der Warenausgabe (30) und dem Warenausgabeterminal (10) vorgesehen ist.

5. Verfahren für eine sichere Datenübertragung beim Verkauf von Waren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet,

dass die Datenübertragung zwischen den einzelnen Bereichen des Warenauswahlbereiches 1, des Kassenbereiches 2, des Warenausgabebereiches 3, mittels Informationsträgern und/oder Vorrichtungen, vorgesehen ist, die drucktechnisch, funktechnisch, lichttechnisch oder magnetisch erfolgt.

HARTING Vending GmbH & Co. KG
Marienwerderstr. 3
D-32339 Espelkamp

2001-07-30
200-14 EP P 4

Verfahren für eine sichere Datenübertragung beim Warenverkauf

Zusammenfassung:

Für den Erwerb von Waren, bei dem die Auswahl der Waren und deren Ausgabe in räumlich getrennten Bereichen realisiert ist, wird ein Verfahren für eine nachahmungssichere Übertragung von warenspezifischen Daten mittels eines oder mehrerer Informationsträger vorgeschlagen. Dabei sind die Informationsträger als (Papier-) Beleg, Transponder, Chip oder Chipkarte (Smart-Card) ausgebildet, wobei voneinander unabhängige, selbstprüfende Verschlüsselungskodes auf jedem der Informationsträger eine korrekte Warenausgabe gewährleisten.

Dokument enthält Seite

Bezugszeichenliste 30.07.2001

Verfahren für eine sichere Datenübertragung

Az.: 200-14 EP P 4

1	Warenauswahlbereich	42	E / A Warenauswahlterminal
2	Kassenbereich	44	E / A Warenausgabespeicher
3	Warenausgabebereich		
10	Warenauswahlterminal		
12	CPU		
14	Belegdrucker	27	
16	Beleg	28	
		29	
20	Kasseneinrichtung	30	
22	Belegleser	31	
24	Ausgabeeinrichtung	32	
26	Informationsträger	33	
28, 28'	CPU	34	
		35	
30	Warenausgabespeicher	36	
32	Leseeinheit	37	
34	Waren	38	
		39	
40	Datenübertragungsstrecke	40	

Copy provided by USPTO from the PIRS Image Database on 04/22/2004